CoinBlesk - a real-time, bitcoin-based payment approach and app

Bocek, Thomas ; Rafati, Sina ; Rodrigues, Bruno ; Stiller, Burkhard

Coinblesk – A Real-time, Bitcoin-based Payment Approach and App

by Thomas Bocek, Sina Rafati, Bruno Rodrigues and Burkhard Stiller (University of Zürich)

The Communication Systems Group (CSG) of the University of Zürich has been exploring the use of blockchains in several application areas. The work concluded that for practical use, Bitcoin transactions should be gathered in a batch.

Generally, blockchains pave the path towards secure data storage in a decentralised manner. They are applicable to a wide range of application domains, such as financial technologies, public registries, and Internet-of-Things (IoT) [1]. As one of the most prominent blockchain examples, Bitcoin has attained large public and research interest, since it offers the first solution for a secure and fully decentralised crypto-currency. Thus, the Communication Systems Group (CSG) of the University of Zürich decided to focus research work on (a) real-time payments with Bitcoins [2, 3], which was trialled at the UZH Mensa [L1] and presented at public fairs [L2], (b) the use of blockchains within IoT, especially the supply chain in the pharmaceutical industry which is highly regulated, and (c) blockchain-based countermeasures for Distributed Denial-of-Service (DDoS) attacks by utilising Smart Contracts (SC).

Blockchain technology has become popular for multiple use-cases, such as IoT, crypto-currency, and security, because blockchains are inherently backed by Smart Contracts. They are defined as formalised protocols to facilitate, verify, or enforce the negotiation or performance of a contract. In this sense, Bitcoin, considered as the pioneer implementation of blockchains, and especially the Bitcoin Script, serve as the first SC for this crypto-currency. Besides theoretical work, the trial deployment of blockchains and their application-specific combination with SCs deliver valuable insights for distributed systems' operations. Specific blockchain benefits include a fully decentralised system operation, transaction transparency, immutability, and security combined with selected areas of legally binding interactions.

In this context the new Coinblesk approach [2, 3, L1, L2] belongs to the use-cases of crypto-currencies. It is an instant payment wallet with Bitcoins and minimal trust with the strategic goal to generalise and optimise its payment protocol to support other crypto-currencies, while maintaining security, privacy, and convenience as key. The CoinBlesk app for Android includes a Bitcoin payment server, where the seller and the buyer are able to handle Bitcoin payments. This safe and fast mobile payment method is contactless, using Near Field Communications (NFC) technology, without the need for swiping, signing, or PIN. To reach a transaction delay below one second, a multisig (multi signature) mechanism was designed such that the Coinblesk server cannot transfer funds without the signature of the client. Since sending every transaction immediately to the blockchain reveals the current limitations of Bitcoins, and the current fee of an average transaction is more than US $2, these transactions are batched and transaction fees are reduced by performing the clearing operation at the server, where the user can specify an amount stipulating when clearing should be made. Only once that amount is reached, is a transaction sent to the Bitcoin blockchain. Thus, if a transaction is cleared on the server (not yet sent to the Bitcoin blockchain) a virtual balance is maintained in order to acknowledge the payment within this one second limit.

This mechanism reduces the number of transactions – termed "batching transactions" – sent to the Bitcoin blockchain and, thus, lowers the average transaction fees of these transactions. The system has been built in such a way that the user

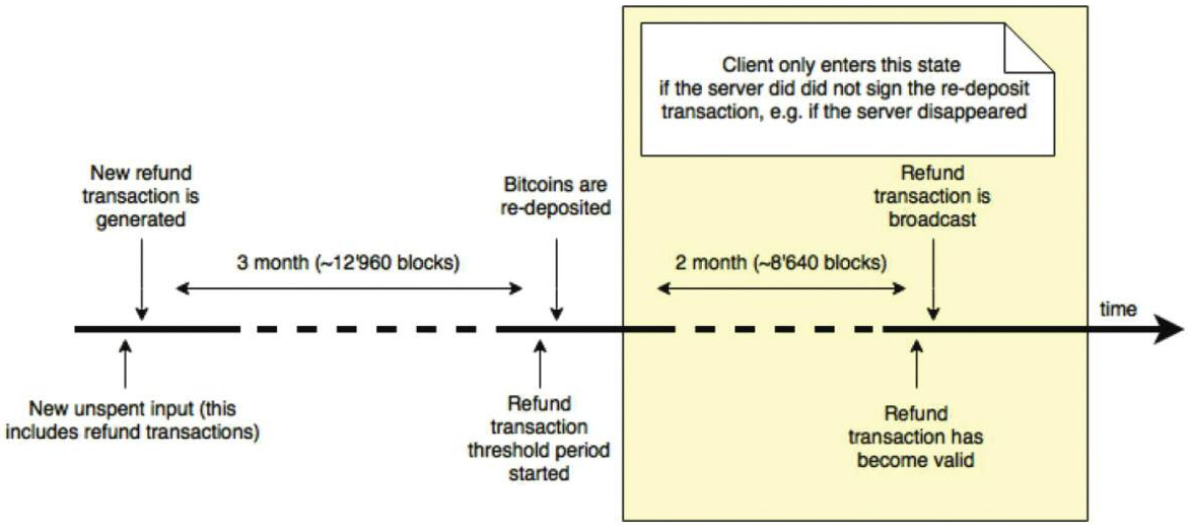

Figure 1: Coinblesk's refund transaction time-line.

can set that maximum amount, since only the user can determine the trust level to be reached. In turn, the system has to broadcast these batched transactions to the Bitcoin blockchain, e.g., if the user sets the limit at €100 and if the virtual balance reaches this value, all accumulated transactions are broadcast. This approach was chosen over the Lightning network's approach [L4], since its technical complexity is lower and more importantly it also works with transaction malleability. The current Coinblesk design can be optimised further, once transaction malleability is solved in the Bitcoin network or any another crypto-currency, such as Litecoin, which does not suffer from malleability, is used. However, as mentioned above, the Coinblesk app does not follow the fully trustless approach in such cases, since the Coinblesk server requires this minimal trust up to the amount specified by the user.

All funds deposited in Coinblesk are held at a 2-of-2 multisig address, which means that even if the operator of the Coinblesk server is intentionally malicious, he will never be able to steal a user's funds. In the case of a Coinblesk server hacking and private keys being stolen, the hacking could only be successful if hackers were able to gain access to the user's private keys as well in order to steal bitcoins. Also, if the Coinblesk server disappears, clients are no longer able to spend their bitcoins. This is a major problem, because Swiss law requires customers of a payment service to be able to gain full access to their funds in any situation, and especially if the operator of a payment system should become bankrupt – or in the case of the Coinblesk service, it might be hacked. Additionally, all Coinblesk clients need to trust that the system will not disappear.

Thus, the effective solution to this problem is a "refund transaction" as time-lined in Figure 1. A refund transaction is a pre-signed, time-locked transaction, which sends all client funds to an address, exclusively controlled by that client. Therefore, a refund transaction is automatically created by the Coinblesk app as soon as a new unspent output appears in the wallet – in particular, whenever bitcoins are received or a transaction is created. The app takes all the unspent outputs and creates a single transaction sending all bitcoins to an address of a private key that is derived from the client's private seed. The client signs this transaction and returns it to the server. The server checks that the transaction is in fact time-locked, signs it, and returns the transaction fully signed back to the client. Now, the client is in possession of a valid, fully signed refund transaction that becomes valid as soon as the time-lock expires. Thus, in case the Coinblesk server suddenly disappears, a client can broadcast the refund transaction and regain control over all their bitcoins.

In conclusion, the experience with the Coinblesk design and implementation as well as experience from other applications, such as the pharmaceutical supply chain [L3, L5], provides useful information about scalability, energy efficiency, ease-of-use, and some insights into customer acceptance. These results should be widely applicable in the blockchain world.

Links:

[L1] http://www.csg.uzh.ch/csg/en/news/Bitcoins.html
[L2] http://www.csg.uzh.ch/csg/en/news/ coinbleskatCeBIT.html
[L3] http://www.csg.uzh.ch/csg/en/news/kickstart-accelerator.html
[L4] https://lightning.network/lightning-network-paper.pdf
[L5] https://modum.io/

References:

[1] T. Bocek, B. Stiller: "Smart Contracts – Blockchains in the Wings", in: C. Linnhoff-Popien, R. Schneider, M. Zaddach (Edts.): "Digital Marketplaces Unleashed", Springer, 2017.
[2] A. D. Carli: "Protocol Improvements in CoinBlesk – A Mobile Bitcoin Instant Payment Solution", Master Thesis, Univ. Zürich, Department of Informatics, Communication Systems Group, Zürich, Switzerland, April 2016.
[3] R. Voellmy: "CoinBlesk, a Mobile NFC Bitcoin Payment System", Bachelor Thesis, Univ.Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, August 2015.

Please contact:

Thomas Bocek, Sina Rafati, Bruno Rodrigues, Burkhard Stiller
University of Zürich, Switzerland
[bocek|rafati|rodrigues|stiller]@ifi.uzh.ch

Bitcoin Unchained

by Christopher Carr, Colin Boyd (NTNU), Xavier Boyen and Thomas Haines (QUT)

Bitcoin's distributed ledger is an innovative way of solving the double spending problem in a decentralised system. However, it causes incompressible transaction delays and incentivises consolidation of mining power. We ask, is it possible to eliminate these problems without losing the decentralised principles that Bitcoin was built on?

Over eight years have gone by since Bitcoin's deployment, and it is still going strong. While there are many explanations for its success, the innovative backbone structure – the blockchain -– which has inspired so many alternative systems, undoubtedly plays a leading role in this story.

Blockchains store the state of the transactions in the system. Users compete to form new blocks, which confirm both new and all existing transactions in the previous blocks. Those who create blocks first are rewarded with cash in the system.

Despite the blockchain innovation, there are some fundamental problems that lie in its design, which stem from the blockchain itself, and affect all similar systems.

Two major problems which are inherent to almost all blockchain models are: